

Approved March 25, 1997
Revised Effective April 17, 2001

NAPA COUNTY INFORMATION TECHNOLOGY USE & SECURITY POLICY

I. STATEMENT OF POLICY

Napa County has a significant investment in networked and on-line personal computer technology in order to assist employees in performing their jobs as efficiently as possible. In addition, advancements are being made to integrate voice and facsimile communications capabilities into the County's personal computer and network technology. As a result County employees are expected to ensure that computers, software, electronically stored data, facsimile, voice-mail equipment and other telecommunications systems are secure and used appropriately. This Policy is intended to apply to all County Information Systems equipment and devices, such as, personal computers, laptops, telephones, cellular phones, facsimile machines, hand-held devices and personal data assistants ("PDAs"). For further guidance, please refer to the Information Technology Use & Security Guidelines.

A. Purpose of Policy

1. To Establish Appropriate Use and Security Guidelines

The County makes every effort to provide employees with the best technology available to conduct the County's official business. Therefore, this policy has been created to advise all users regarding the appropriate use of, access to, and the disclosure of information created, transmitted, received and stored via the use of County computing and telecommunications networks, systems and equipment (collectively referred to as Napa County's Information Systems) and is intended to guide employees in the performance of duties as related to the use of these Information Systems. All employees and other users are required to adhere to this Policy. Certain departments may have unique requirements and are encouraged to develop separate policies and guidelines to address those issues.

2. To Provide Notice Regarding Expectation of Privacy

This Policy is also intended to notice employees that all County Information Systems, and their contents, are not confidential or private. That is, all data, including any that is stored electronically or printed as a document, is subject to audit, review, disclosure and discovery. **Such data may be subject to disclosure pursuant to the Public Records Act (California Government Code Section 6250 et. seq.). Therefore, there is no expectation of privacy in the use of the County's Information Systems.**

Accordingly, the County reserves the right to access and monitor employee use of the County's Information Systems as well as any stored information, created or

received by County employees, with the County's Information Systems. The reservation of this right is to ensure that the County's Information Systems are used securely and appropriately in an ethical and lawful manner.

3. Applicability of This Policy to Other County Information Systems Users

Persons providing services to the County pursuant to a contract, vendors, or others who use the County's Information Systems during the course of performing their duties, will be held accountable for abiding by this Policy.

II. USE OF COUNTY INFORMATION SYSTEMS

A. General Use Statement

As improvements in County technology provide increased connectivity, the actions of one employee can impact the integrity and security of a telecommunications network used by many. A County employee, or any other user granted use of the County's Information Systems is expected to use those systems in a responsible manner by complying with all policies, relevant laws and contractual agreements.

All County Information Systems furnished to employees as well as to any other users, are Napa County property, intended for County business use. Use of County Information Systems for personal or commercial gain is prohibited. As a condition of employment, all employees will be required to sign a Standard of Conduct Agreement to acknowledge that they have read and understand this Policy, and, by so signing, consent to the County's accessing, reviewing and disclosing data or messages stored in the County's Information Systems. Department Heads are responsible for taking appropriate action for any violations of this policy.

These same Policy provisions, as well as other applicable County policies, apply to employees and any other users who access the County's Information Systems from remote sites.

B. Prohibited Use

The use of the County's Information Systems is restricted to "official County business", therefore, certain conduct is considered to be in violation of the County's Information Technology Use & Security Policy. In addition, such prohibited use may be in violation of other applicable County policies. Examples of prohibited use include, but are not limited, to the following:

- Personal use of or time spent for personal gain which exceeds incidental use.

- Using the County network to gain unauthorized access to other areas of the County system or other systems to which the County is connected. Such an action is a violation of this Policy as well as the Federal Electronic Communications Privacy Act (ECPA) 18 U.S.C. § 2510.
- Attempting to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secured data.
- Knowingly or carelessly running or installing on any computer system or network, programs known as computer viruses.
- Violating terms of applicable software licensing agreement or copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images etc.
- Using County resources for private commercial activity such as creating products or reports for sale.
- Using electronic mail to harass or threaten others. This includes sending repeated, unwanted e-mail to another user.
- Using the Computer or Internet for political campaigns.
- Transmitting or reproducing materials that are vulgar, lewd, disturbing or sexually explicit or that otherwise violate existing County policy.
- Transmitting or reproducing materials that are slanderous or defamatory in nature or that otherwise violate existing County policy.
- Representing yourself as someone else, real or fictional, or sending a message anonymously.
- Downloading files from the Internet without first scanning them with the County's standard virus prevention software.
- Sending, posting or providing access to any sensitive or confidential County material or information unless for official County business purposes.
- Any violation of this Policy may result in disciplinary action up to and including termination as well as civil and/or criminal prosecution.

III. COUNTY INFORMATION SYSTEMS DATA ACCESS**A. Right of Access**

1. The County has an unrestricted right of access to, inspection of, and disclosure of all voice and electronic data and software on any County equipment or media, at the request of appropriate County management. Such access and disclosure shall be in accordance with, and subject to any controls or restrictions imposed by applicable statutes or licenses, and in a manner consistent with preservation of evidentiary privileges.
2. Access to and review of voice and electronic data and Internet files on County Information Systems or media will follow supervisory lines. The supervisor and higher authorities under whom each staff member, other user, or official, works has the authority to access, inspect and disclose information, in accordance with the policies contained in this section, and consistent with applicable statutes or licenses. Peers and subordinates have no authority to access or disclose except as specifically granted by Department manager.

B. Obligation to Provide Access

Individual County employees, officials, or other users of County Information Systems or media are required to immediately provide access, decrypt and disclose any passwords, files or data to appropriate County management upon request. (All County employees, officials and other users shall be informed of this requirement and required to sign and acknowledge the Information Technology Use Standard of Conduct Agreement)

IV. SOFTWARE AND DATA OWNERSHIP**A. County of Napa Ownership Rights**

1. Ownership rights for all software owned or controlled by the Napa County are vested in the "County of Napa" and are subject to the controls, policies, and procedures established by the Board of Supervisors, except where otherwise provided by software license or consultants under a contract. All software and documentation developed by or under the supervision (direct or indirect) of County programming personnel during work hours or using County Information Systems is the property of the County, until such time that the County abandons or transfers ownership except where such ownership or work is governed by an existing contract or agreement.
2. Data files are public records under the control of the appointed Custodians of Records for the respective County Departments, appointed or elective offices.

Ownership and control of such information shall be consistent with the California Public Records Act. The fact that individual items or collections of data or software are public in nature, or actually are public records, does not diminish the “property” aspects of County ownership.

3. The County may, in its sole discretion, assert, establish and exercise property rights in any and all data, files and software stored, maintained, created or placed on any County Information Systems including transferable media such as diskettes and tapes, unless that file or software is the licensed property of another entity. The assertion, establishment, and exercise of such rights may occur at any level along lines of supervisory authority. Such action shall be in a manner consistent with state and federal laws. Request for review of such action shall be to the applicable Department Head, whose decision is final.
4. The Department of Information Technology Services (ITS) has custodial responsibility for software licensing and data security administration. This includes all data and programs supporting network systems including the processing and storage of data for County Departments.

V. STATUS OF OTHER POLICIES

This policy supercedes and replaces all other policies on the same subject, especially that policy entitled, “NAPA COUNTY COMPUTER INFORMATION & SECURITY POLICY” adopted by the Board of Supervisors effective on or about March 25, 1997. The County reserves the right to amend or append this policy to include necessary guidelines for new developments in computer information use, such as storage of e-mail and stored data and integrated telecommunications systems with computer and electronic data systems, or whenever it is appropriate to conform to state and federal laws, rules and regulations.

<p>NAPA COUNTY Information Technology Use & Security Policy STANDARD OF CONDUCT AGREEMENT</p>

BY SIGNING THIS FORM, I UNDERSTAND AND AGREE TO THE FOLLOWING:

This is to certify that I have read and understand and agree to abide by the Napa County Information Technology Use and Security Policy.

I understand that as a County employee or person who provides services to the County, I have access rights only to the information with which I have been assigned to work and that accessing confidential information in files or other stored communications data other than those to which I am assigned to work, or using County equipment or on-line services to access and/or distribute to other County employees, contractors or members of the public, any unacceptable information obtained from any source, is expressly prohibited.

I understand that the County maintains the right to monitor, access, examine and disclose all data and information stored and transmitted by a County computer and/or telecommunications system in accordance with applicable laws and policies in order to ensure the proper use and maintenance of these systems.

I further understand that failure to comply with any of the guidelines and requirements of the Napa County Information Technology Use and Security Policy, as well as other related County Policies and state and/or federal law could result in disciplinary action, up to and including termination of my employment.

I also agree to periodically review the associated Information & Technology Use & Security Guidelines. In addition, changes or modifications may be made to this Policy and I understand that the law, this Policy and associated Guidelines regarding the use of the County's information systems are continually evolving. Therefore, I understand that my regular review of this Policy is required. I understand that updates to this Policy and associated Guidelines will be made available to me when changes or modifications to these occur.

This acknowledgement form will be filed in my personnel file and with the Department of ITS.

EMPLOYEE ACKNOWLEDGMENT:

Employee Name (print)

Signature

Employee's Department

Date